PATENT ABSTRACTS OF JAPAN

(11)Publication number : 61-029232
(43)Date of publication of application : 10.02.1986

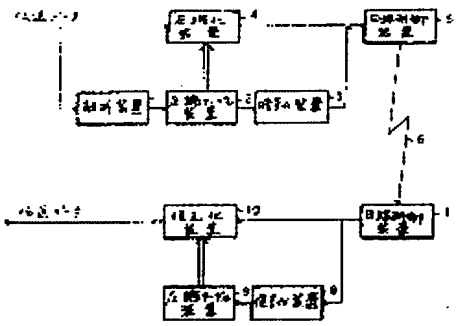
(51)Int.Cl. H04L 9/00
H04L 23/00

(21)Application number : 59-149416
(22)Date of filing : 20.07.1984

(71)Applicant : HITACHI LTD
(72)Inventor : SHIMOZAKA TOSHIAKI
OKADA JUN
KUNIMASA KOICHI

(54) DATA ENCIPHERMENT TRANSMISSION SYSTEM

(57)Abstract:
PURPOSE: To secure the safety of data and to improve the data transmission efficiency by compressing the transmission data by a compression table, enciphering the compression table to transmit it together with the data and decoding the enciphered compression table at the reception side to restore the compressed data.
CONSTITUTION: An analyzer 1 analyzes the character emerging frequency of the transmission data, and a compression table device 2 produces and stores a compression table suited to the compression processing of data based on the result of analysis of the analyzer 1. This compression table is enciphered by an enciphering device 3 and sent to a circuit 6 through a circuit controller 5. While a compressing device 4 compressed the compression data via the compression table of the device 2 and sends it to the circuit 6 through the controller 5 after the enciphered compression table. At the reception side, a circuit controller 7 decodes the enciphered compression table in the reception data through a decoder 8 to obtain a compression table. This table is stored to a compression table device 9. Then the compressed data is restored to the original data by a restoring device 10 by means of the compression table sent from the device 9.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's

decision of rejection]
[Date of extinction of right]

⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　昭61－29232

⑤1Int.Cl.⁴	識別記号	庁内整理番号	⑬公開　昭和61年(1986)2月10日
H 04 L 9/00		7240－5K	
23/00		7240－5K	

審査請求　未請求　発明の数 1　（全4頁）

⑤4発明の名称　データ暗号化伝送方式

⑳特　願　昭59－149416
㉒出　願　昭59(1984)7月20日

⑦2発明者　下坂　俊明　秦野市堀山下1番地　株式会社日立製作所神奈川工場内
⑦2発明者　岡田　純　秦野市堀山下1番地　株式会社日立製作所神奈川工場内
⑦2発明者　国正　興一　秦野市堀山下1番地　株式会社日立製作所神奈川工場内
⑦1出願人　株式会社日立製作所　東京都千代田区神田駿河台4丁目6番地
⑦4代理人　弁理士　高橋　明夫　外1名

明　細　書

1．発明の名称

データ暗号化伝送方式

2．特許請求の範囲

(1) 送信側において、伝送データを圧縮テーブルを用い圧縮して伝送するとともに、その圧縮テーブルを暗号化して伝送し、受信側において、暗号化圧縮テーブルを復号化して元の圧縮テーブルを得、その圧縮テーブルを用いて圧縮伝送データから伝送データを復元することを特徴とするデータ暗号化伝送方式。

3．発明の詳細な説明

〔発明の利用分野〕

本発明は、データ暗号化伝送方式に関する。

〔発明の背景〕

データ伝送の安全性を高めるために、種々のデータ暗号化伝送方式が考えられている。しかし従来の方式は、伝送データを全て暗号化して伝送し、受信側において暗号化伝送データを復号化するため、暗号化および復号化の処理時間が長く、また暗号化により伝送データ長が増加し、その結果、データの伝送効率が悪いという欠点があった。

伝送データ長を短縮するために、暗号化伝送データをデータ圧縮する方式もあるが、そのような圧縮処理を行っても、暗号化しない場合に比べデータ伝送効率がかなり悪化する。

〔発明の目的〕

本発明の目的は、従来と同等のデータ伝送の安全性を達成し、かつ従来よりも伝送効率を改善できるデータ暗号化伝送方式を提供することにある。

〔発明の概要〕

本発明によれば、伝送データは暗号化することなくそのままデータ圧縮して伝送し、一方、伝送データの圧縮の用いる圧縮テーブルを暗号化して伝送する。受信側においては、暗号化圧縮テーブルを復号化して元の圧縮テーブルを得、その圧縮テーブルを用いて圧縮伝送データから元の伝送データを復元する。即ち、圧縮テーブルの秘密の鍵として利用し、その圧縮テーブルを暗号化して伝送することにより、伝送データ長および暗号化・

復号化処理時間の短縮を図ると同時に、伝送データ全体を暗号化すると同等のデータに安全性を達成するものである。

〔発明の実施例〕

第１図は本発明の一実施例を示すブロック図である。この図において、１～５は送信側の装置であり、７～１０は受信側の装置である。６は回線である。

送信側において、解析装置１は伝送データの出現文字の頻度を解析し、その解析結果に基づいて圧縮テーブル装置２は伝送データの圧縮処理に適した圧縮テーブルを作成し、内部に記憶する。暗号化装置３は、圧縮テーブル装置２によって作成された圧縮テーブルまたは圧縮テーブルの変更情報（後述）を暗号化する。その暗号化圧縮テーブルは、回線制御装置５を通して回線６へ送出される。一方、圧縮化装置４は、圧縮テーブル装置２によって作成された圧縮テーブルを用いて、伝送データをデータ圧縮する。その圧縮伝送データは、暗号化圧縮データに続いて、回線制御装置５を通じて回線６へ送出される。

受信側において、回線６を通じて伝送されてくる暗号化圧縮テーブルと圧縮伝送データを回線制御装置７を通じて受信する。復号化装置８は、受信した暗号化圧縮テーブルを復号化し、伝送データの圧縮処理に用いられた圧縮テーブルを得、それを圧縮テーブル装置９に記憶させる。復元化装置１０は、圧縮テーブル装置９に記憶されている圧縮テーブルを用い、受信された圧縮伝送データから圧縮前の伝送データを復元する。

送信側の解析装置１および圧縮テーブル装置２について、第２図によりさらに説明する。この図に示すように、解析装置１においては、一定間隔毎に伝送データ中の文字の出現回数を頻度測定装置１１により測定し、その測定結果に従って頻度順変更装置１２で各文字を頻度順に並べ換える。圧縮テーブル装置２は、圧縮テーブル記憶装置１４と圧縮テーブル変更装置１３からなる。本実施例においては、データ圧縮をハフマン符号化法によって行うようになっており、伝送開始前は、第４図に例示するようなハフマンコードに対応する未割当て状態の圧縮テーブルが圧縮テーブル記憶装置１４に記憶されている。伝送開始時には、解析装置１による解析結果と、圧縮テーブル記憶装置１４に記憶されている未割当て状態の圧縮テーブルにより、圧縮テーブル変更装置１３は圧縮テーブルの割当てを行い、割当て後の圧縮テーブルを圧縮テーブル記憶装置１４に記憶させるとともに、暗号化装置３へ送る。

圧縮テーブルの作成に当っては、第４図の例示するように、文字の割当てを行い、「空」の部分を各頻度毎に１～数箇所作っておく。伝送中において一定間隔毎に頻度が測定され、頻度順変更装置１２から解析結果が出る。圧縮テーブル変更装置１３は、圧縮テーブル記憶装置１４にある圧縮テーブルの頻度順と、頻度順変更装置１２によって与えられる頻度順とを比較し、頻度が変更になった文字の再割当てを実施する。この再割当ては、変更文字の変更前の圧縮テーブルの変更先の頻度にある「空」の部分に割り当てることによって行う。変更後の圧縮テーブルは圧縮テーブル記憶装置１４に記憶される。また圧縮テーブルの変更部分は、暗号化装置３に送られ、暗号化され伝送される。

ここで、本実施例ではキャラクタ対応文字の例を示しているが、他の図形データや画面データ等のビット列の場合、伝送データ中のビット列を一定間隔（たとえば８ビット）毎に区切ることにより、同様に圧縮テーブルを作成することができる。

次に第３図を参照して、受信側の圧縮テーブル装置９についてさらに説明する。圧縮テーブル未設定時は、復号化装置８で復号化された圧縮テーブルが、圧縮テーブル変更装置１５により復元化用に修正されて圧縮テーブル記憶装置１６に格納される。伝送中においては、圧縮テーブルの変更情報が伝送されて来た場合、復号化装置８で復号化して圧縮テーブル変更装置１５に送る。圧縮テーブル変更装置１５は、復号化装置８から与えられる変更情報により、圧縮テーブル記憶装置１４に記憶されている圧縮テーブルを変更する。

なお、上記実施例においては、伝送データを一伝間隔毎に、つまり一定伝送文字数毎に解析し、圧縮テーブルを変更しているが、伝送前に伝送データの全部または一部を予め解析し、その解析結果に従って圧縮テーブルを作成し、以後その圧縮テーブルを継続して使用するようにしてもよい。この場合、伝送中においては圧縮テーブルが変更されることはないから、圧縮テーブルの変更情報を暗号化して送る必要はなくなる。

また、データ圧縮法は、上述のハフマン符号化法に限られるものではない。

〔発明の効果〕

以上詳細に説明したように、本発明のデータ暗号化伝送方式は、送信側において、伝送データを暗号化するのではなく、圧縮テーブルを暗号化し、暗号化圧縮テーブルと圧縮伝送データとを伝送し、受信側において暗号化圧縮テーブルを復号化し、復号した圧縮テーブルを用いて圧縮伝送データを元の伝送データに復元する方式であるから、伝送データ全体を暗号化および復号化する従来方式に比べ、暗号化および復号化処理の時間が大幅に短縮され、また伝送データ長も短縮されるため、データの安全性と伝送の効率化を同時に満足させることができる。

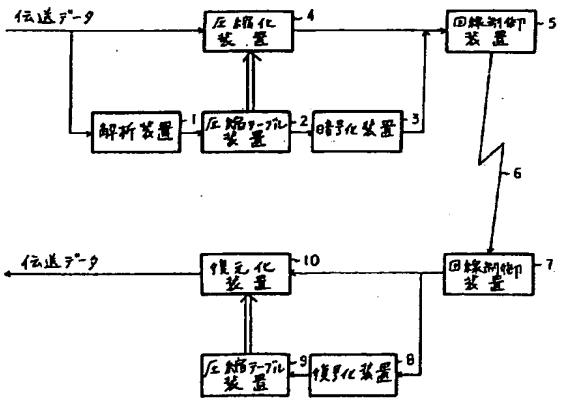
4．図面の簡単な説明

第1図は本発明の一実施例を示す概略ブロック図、第2図は送信側の解析装置および圧縮テーブル装置のブロック図、第3図は受信側の圧縮テーブル装置のブロック図、第4図はハフマンコードの例を示す図である。

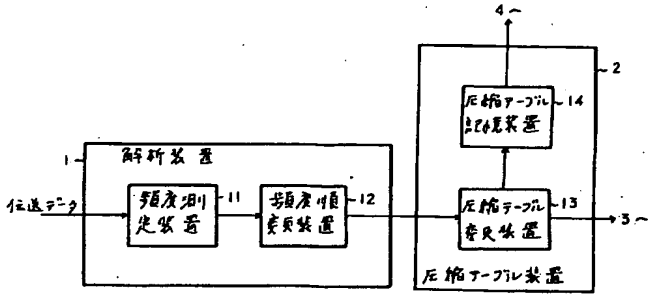
1…解析装置、　2，9…圧縮テーブル装置、
3…暗号化装置、　4…圧縮化装置、
5，7…回線制御装置、　6…回線、
8…復号化装置、　10…復元化装置、
11…頻度順測定装置、　12…頻度順変更装置、　13，15…圧縮テーブル変更装置、
14，16…圧縮テーブル記憶装置。

代理人弁理士　高　橋　明　夫

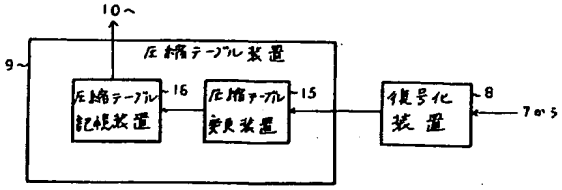
第1図



第2図



第3図



第 4 図

符号長	出現順序	文字	ハフマン・コード
4	1	の	0000
	空	一	0001
5	2	、	00100
	3	に	00101
	空	一	00110
	〃	〃	〃
6	4	る	010000
	5	は	010001
	〃	〃	〃
	空	一	010101
	〃	〃	〃
〃	〃	〃	〃
12	501	毛	111101000001
	502	竜	111101000010
	503	穴	111101000011
	〃	〃	〃
	空	二	111111111011
	〃	〃	〃
〃	〃	〃	〃